CLAIMS

1. Method for registering users of a public-key infrastructure based on credentials of a user, including biometric data such as data related to a fingerprint, presented to an authority (100) of the public-key infrastructure, comprising the steps of

a) connecting a token (10),

which comprises a processor (2), an interface device (3) and a memory device (5), containing a private-key (51) and a public-key (52) for the user of the token (10) and a private-key (53) issued by the authority (100);

to a terminal (20, 30) capable to access the network (200) of the public-key infrastructure,

b1) reading biometric data (58) of the user, such as data derived from a finger print of the user, by a biometric input device (1; 31);

b2) signing the biometric data (58) with a key of an asymmetric or symmetric key pair or by means of a shared password issued by the authority (100);

b3) sending a certification request, containing the public-key (52), signed biometric data (58) and additional credentials of the user, to the authority (100);

c1) verifying and registering the received data by the authority (100);

c2) storing the biometric data (58) in a database (104);

c3) returning a corresponding certificate (520) and

d) storing the certificate (520) in the token.

2. Method according to claim 1 comprising the steps of double signing the biometric data with said key of an asymmetric or symmetric key pair or by means of a shared password and the user's private key (51).

3. Method according to claim 1 or 2, with a serial number of the token being stored in the memory device (5), which, included in the certification request, is sent to the authority (100) which, based on said serial number, retrieves the symmetric or asymmetric key or the password matching the key or password used for signing the biometric data (58) in order to decrypt the signed message.

4. Method according to claim 1, 2 or 3 for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising the steps of issuing for each token (10) an individual symmetric or asymmetric key-pair, a first key stored in the token (10) for signing the biometric data (58) and a second key (54) stored at the registration authority (101).

5. Method according to claim 1, 2, 3 or 4 with the public-key (54; 55) of the registration authority (101) and or the certification authority (102) being stored in the token (10), comprising the steps of encrypting at least the part of the certification request containing the biometric data with one of said public-keys (54; 55) before sending it and decrypting the received certification request by the registration authority (101) with the corresponding private-key (53, …).

6. Method according to one of the claims 1-5 with the biometric input device (31) being integrated in the token (10) comprising the steps of pressing a finger onto the token (10) while biometric data (58) is read.

7. Method according to one of the claims 1-6 comprising the steps of storing the biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

8. Method according to one of the claims 1 to 7 comprising the steps of comparing a password entered with the password stored in the token (10) and/or reading biometric data from the user and comparing biometric data read ,with biometric data (58) stored in the token (10) or in the database (104) of the authority (100) and providing access to the system in case that the compared data match and/or storing mismatched data as proof for legal prosecution of a non-authorised user of the token 10.

9. Method according to one of the claims 1 to 8 comprising the steps of generating the key pair for the user, the private-key (51) and the public-key (52) within the token (10).

10. Method according to one of the claims 1 to 9 comprising the steps of performing transactions defined by the authority of the public-key infrastructure while using the registered token (10).

11. Method according to one of the claims 1 to 10 comprising the steps of keeping the user's data, particularly the biometric data, private except for cases of fraud.

12. Token (10) designed for registering users at an authority (100) of a public-key infrastructure particularly according to the method of claim 1, comprising a processor (2), a memory device (5), an operating system (4) and an interface device (3) designed for exchanging data with a terminal (20, 30) which is capable to access the network (200) of the public-key infrastructure, **characterised** in that

a) the memory device (5) contains a private-key (51) and a public-key (52) for a user of the token (10) and a private-key (53) issued by the authority (100);

b) the token (10) is capable of processing biometric data (58) read and transferred from an internal or external biometric input device (31);

c) the token (10) is capable of signing the read biometric data (58) with a key of an asymmetric or symmetric key pair or by means of a shared password issued by the authority (100);

d) the token (10) is capable of storing a certificate (520) which has been issued by the authority (100) based upon a certification request originating from the token (10).

13. Token (10) according to claim 12 capable of signing the read biometric data (58) with the key of the asymmetric or symmetric key pair or by means of a shared password and the user's private key (51).

14. Token (10) according to claim 12 or 13, with a serial number of the token being stored in the memory device (5).

15. Token (10) according to claim 12, 13 or 14 for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising an individual key of a symmetric or asymmetric key-pair or a shared password for signing the biometric data (58) and a public-key (55) issued by the registration authority (101) or the certification authority (102) for encrypting the certification request sent to the authority (100).

16. Token (10) according to one of the claims 12-15 with the biometric input device (1) being integrated in the token (10).

17. Token (10) according to one of the claims 12-16 designed to store the read biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

18. Token (10) according to one of the claims 12-17 capable to compare a password entered with the password stored in the token (10) and/or capable of reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) providing access to the system in case that the compared data match.

19. Token (10) according to one of the claims 12-18 capable to generating the key pair for the user, the private-key (51) and the public-key (52), within the token (10).

20. Registration system (35) providing access to a token (10) according to one of the claims 12-19 with a terminal(30) designed to exchange data with the network (200) of the public-key infrastructure, with a connected token (10) and with at least one biometric input device (31) capable of reading biometric data, preferably as data related to a fingerprint, the retina, the face and/or the voice of a user which biometric data is transferable via the terminal (30) to the token (10) for processing.